CLAIMS

What is claimed is:

1. A method of detecting loss of stream cipher synchronization between a transmitter and a receiver in a video processing system comprising:

receiving, by the receiver, an encrypted video frame from the transmitter;

obtaining an encrypted value for a selected pixel in the encrypted video frame;

decrypting the encrypted pixel value using a first portion of the receiver's current key stream;

re-encrypting the pixel value using a second portion of the receiver's current key stream;

sending the re-encrypted pixel value from the receiver to the transmitter;

obtaining, by the transmitter, a plaintext value for the selected pixel from a corresponding original video frame and encrypting the plaintext pixel value using a second portion of the transmitter's current key stream; and

comparing the re-encrypted pixel value received from the receiver with the encrypted pixel value generated by the transmitter and detecting a loss of cipher synchronization when the values do not match.

2. The method of claim 1, further comprising initiating a restart of the stream cipher synchronization when the loss is detected.

3. The method of claim 1, further comprising repeating the detection of loss of stream cipher synchronization for every frame in a stream of video frames.

4. The method of claim 3, further comprising selecting different pixels in each successive frame of the video stream.

5. The method of claim 1, wherein the comparing step is performed by an entity other than the transmitter and the receiver.

6. The method of claim 1, wherein the re-encrypted pixel value is sent from the receiver to the transmitter over a back channel.

7. The method of claim 1, wherein obtaining the encrypted value of the selected pixel and decrypting the encrypted pixel value are performed prior to decrypting the encrypted video frame.

8. An article comprising: a machine readable storage medium storing instructions, that when executed by a processing system detect loss of stream cipher synchronization between a transmitter and a receiver in a video processing system by receiving, by the receiver, an encrypted video frame from the transmitter, obtaining an encrypted value for a selected pixel in the encrypted video frame, decrypting the encrypted pixel value using a first portion of the receiver's current key stream, re-encrypting the pixel value using a second portion of the receiver's current key stream, sending the re-encrypted pixel value from the receiver to the transmitter, obtaining, by the transmitter, a plaintext value for the selected pixel from a corresponding original video frame and encrypting the plaintext pixel value using a second portion of the transmitter's current key stream, and comparing the re-encrypted pixel value received from the receiver with the encrypted pixel value generated by the transmitter and detecting a loss of cipher synchronization when the values do not match.

9. The article of claim 8, further comprising instructions for initiating a restart of the stream cipher synchronization when the loss is detected.

10. A method of detecting loss of stream cipher synchronization between a transmitter and a receiver in a video processing system comprising:

receiving, by the receiver, an encrypted video frame from the transmitter;

obtaining an encrypted value for a selected pixel in the encrypted video frame;

decrypting the encrypted pixel value using a first portion of the receiver's current key stream;

sending the decrypted pixel value from the receiver to the transmitter;

obtaining, by the transmitter, a plaintext value for the selected pixel from a corresponding original video frame; and

comparing the decrypted pixel value received from the receiver with the plaintext pixel value obtained by the transmitter and detecting a loss of cipher synchronization when the values do not match.

11. An article comprising: a machine readable storage medium storing instructions, that when executed by a processing system detect loss of stream cipher synchronization between a transmitter and a receiver in a video processing system by receiving, by the receiver, an encrypted video frame from the transmitter, obtaining an encrypted value for a selected pixel in the encrypted video frame, decrypting the encrypted pixel value using a first portion of the receiver's current key stream, sending the decrypted pixel value from the receiver to the transmitter, obtaining, by the transmitter, a plaintext value for the selected pixel from a corresponding original video frame, and comparing the decrypted pixel value received from the receiver with the plaintext pixel value obtained by the transmitter and detecting a loss of cipher synchronization when the values do not match.

12. A method of detecting loss of stream cipher synchronization between a transmitter and a receiver in a video processing system comprising:

receiving, by the receiver, an encrypted video frame from the transmitter;

obtaining an encrypted value for a selected pixel in the encrypted video frame;

decrypting the encrypted pixel value using a first portion of the receiver's current key stream;

re-encrypting the pixel value using a second portion of the receiver's current key stream;

sending the re-encrypted pixel value from the receiver to the transmitter;

obtaining, by the transmitter, a plaintext value for the selected pixel from a corresponding original video frame and decrypting the received re-encrypted pixel value using a second portion of the transmitter's current key stream; and

comparing the decrypted pixel value received from the receiver with the plaintext pixel value obtained by the transmitter and detecting a loss of cipher synchronization when the values do not match.

13. An article comprising: a machine readable storage medium storing instructions, that when executed by a processing system detect loss of stream cipher synchronization between a transmitter and a receiver in a video processing system by receiving, by the receiver, an encrypted video frame from the transmitter, obtaining an encrypted value for a selected pixel in the encrypted video frame, decrypting the encrypted pixel value using a first portion of the receiver's current key stream, re-encrypting the pixel value using a second portion of the receiver's current key stream, sending the re-encrypted pixel value from the receiver to the transmitter, obtaining, by the transmitter, a plaintext value for the selected pixel from a corresponding original video frame and decrypting the received re-encrypted pixel value using a second portion of the transmitter's current key stream, and comparing the decrypted pixel value received from the receiver with the plaintext pixel value obtained by the transmitter and detecting a loss of cipher synchronization when the values do not match.

14. A video processing system comprising:

a transmitter adapted to encrypt video frames and to send a stream of encrypted video frames; and

a receiver adapted to receive the stream of encrypted video frames from the transmitter, to obtain an encrypted value for a selected pixel in a selected

encrypted video frame, to decrypt the encrypted pixel value using a first portion of the receiver's current key stream, to re-encrypt the pixel value using a second portion of the receiver's current key stream, and to send the re-encrypted pixel value from the receiver to the transmitter;

wherein the transmitter is further adapted to obtain a plaintext value for the selected pixel from a corresponding original video frame, to encrypt the plaintext pixel value using a second portion of the transmitter's current key stream, to compare the re-encrypted pixel value received from the receiver with the encrypted pixel value generated by the transmitter, and to detect a loss of cipher synchronization when the values do not match.

15. The video processing system of claim 14, further comprising a forward transmission link for sending the stream of encrypted video frames from the transmitter to the receiver and a back channel for sending the re-encrypted pixel value from the receiver to the transmitter.

16. The video processing system of claim 14, wherein the transmitter and receiver each comprise a stream cipher engine for performing encryption and decryption operations.

17. The video processing system of claim 14, wherein the transmitter comprises a compare function to compare the re-encrypted pixel value received from the receiver with the encrypted pixel value generated by the transmitter, and to detect a loss of cipher synchronization when the values do not match.